

区块链存证

信任润滑经济，技术驱动变革

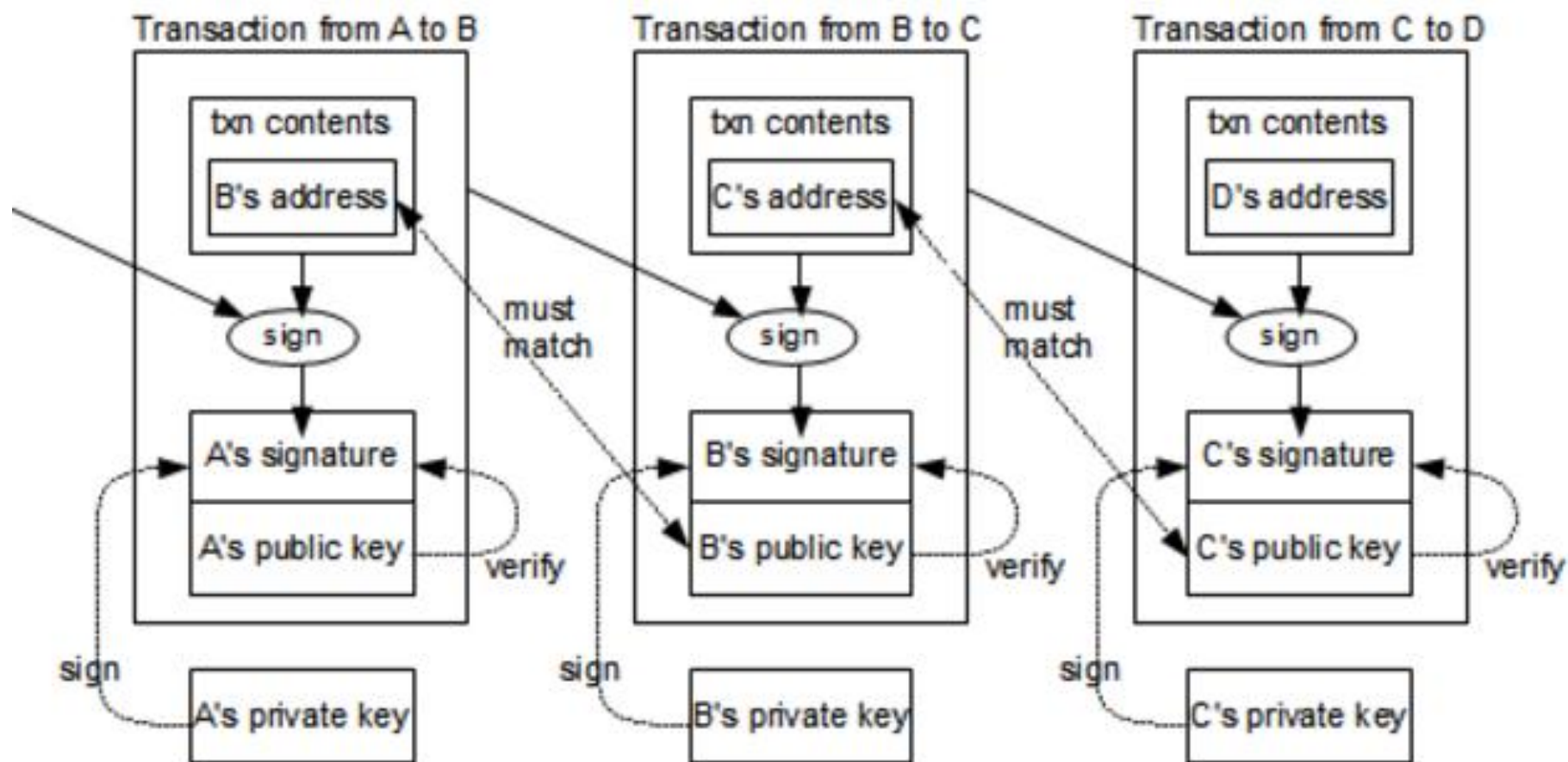
BLOCKCHAIN

汪波

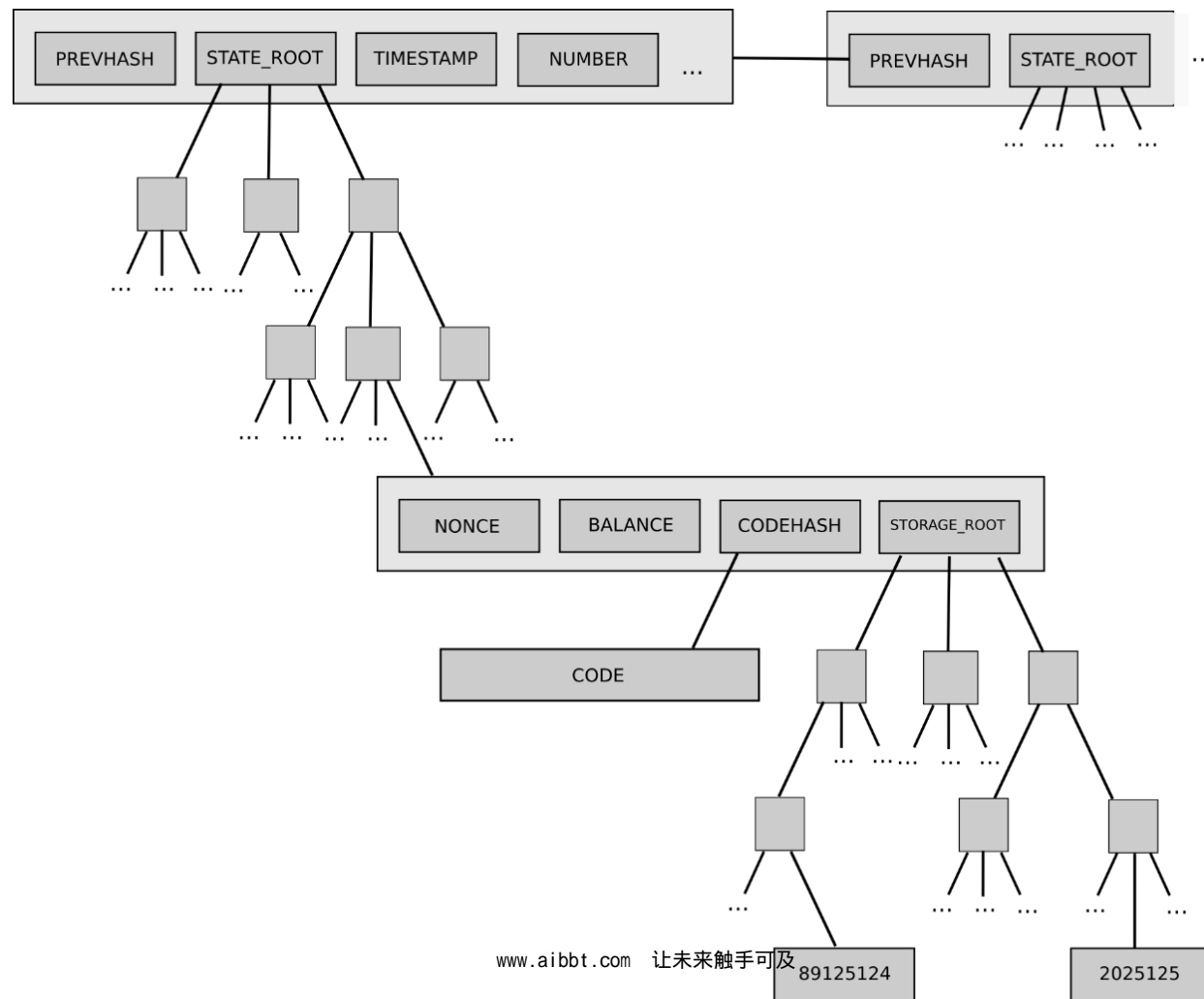
Agenda

- 为什么区块链是一个好的存证工具
- 怎么做存证
- 存证的现状
- 企业级的存证解决方案
- Q & A

区块链作为存证工具：交易结构



存证工具：区块链



存证工具：共识机制

- 共识算法（+ 挖矿）
 - PoW: Proof of Work
 - PoS / DPOS: Proof of Stake
 - PBFT: Practical Byzantine Fault Tolerance
 - Raft
 - Paxos
- 保证了整个区块链不可完全被重写

如何做存证 (Bitcoin) : coinbase

Transaction View information about a bitcoin transaction

4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

No Inputs (Newly Generated Coins)



1A1zP1eP5QGefi2... (Genesis of Bitcoin [link](#)) - (Unspent) 50 BTC

CoinBase

04ffff001d0104

(decoded) ↔

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

72206f6e206272696e6b206f66207365636f6e64206261696c6f757420666f722

Output Scripts

04678afdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649f6bc3f4cef38c4f35504e51ec112de5c384df7ba0b8d578a4c702b6bf11d5f

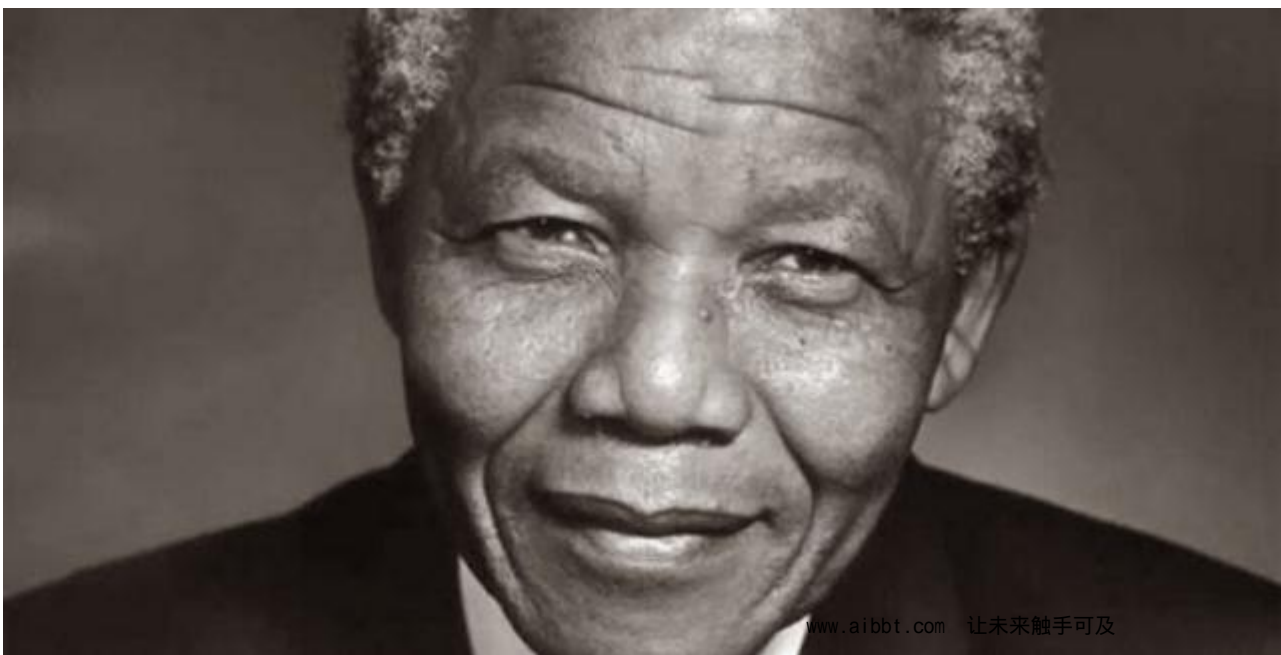
OP_CHECKSIG

OK

如何做存证：btc address

16LseQUKmhA1XUq39QmxNg9c1bPQq6Jxvh (0.157245 BTC - Output) →

1AFZvFuA5Pv3RTw679GFvYbAzykZqm3Ys2 - (Unspent)	0.000055 BTC
1AcHQwytPpRKkX71DQasUk5TMw6qNED2Yqw - (Unspent)	0.000055 BTC
15gHNr4TCKmhHDEG31L2XFNvnpEcnPSQvd - (Unspent)	0.000055 BTC
15VAeb5KsRqbyNWWp7VHSAcuVQahe5ngS7 - (Unspent)	0.000055 BTC
112CUyPHVEi3zyHViBzP3poagnvyUomYZ - (Unspent)	0.000055 BTC
1A8gyj9ETeGkS1hea2crNp1oJ7HfcRMuK8 - (Unspent)	0.000055 BTC
17mkD8JSfeVDx11ZumnEuKo6wVNw9mhipU - (Unspent)	0.000055 BTC



如何做存证：OP_RETURN

Output Scripts

OP_DUP OP_HASH160 1450fb97678094355a5347e046c829e593af4583 OP_EQUALVERIFY OP_CHECKSIG

OP_DUP OP_HASH160 982115cc87baacec85191377b77e22c062073bf2 OP_EQUALVERIFY OP_CHECKSIG

OP_RETURN 48656c6c6f2c207265616c20626c6f636b636861696e21
(decoded) jHello, real blockchain!

Provably prunable, no unspent output

OP_RETURN (0x6a) + 80 bytes

网录锚定 (Anchor)

Output Scripts

```
OP_RETURN 46610000000fd3dad0571dad4b3371adad1a2f6dcc20092e89c43e90ad0020b7400dea170680d5d  
(decoded) j(Fa=qQ7bCt,ph ]
```

```
OP_DUP OP_HASH160 c5b7fd920dce5f61934e792c7e6fcc829aff533d OP_EQUALVERIFY OP_CHECKSIG
```

- Encoding: 'Wa' (2 bytes) + block_height (6 bytes) + block_hash(32 bytes)

```
anchorHash = append([]byte{'W', 'a'}, blockHeight, hash...)
```

```
builder := txscript.NewScriptBuilder()  
builder.AddOp(txscript.OP_RETURN)  
builder.AddData(anchorHash)
```

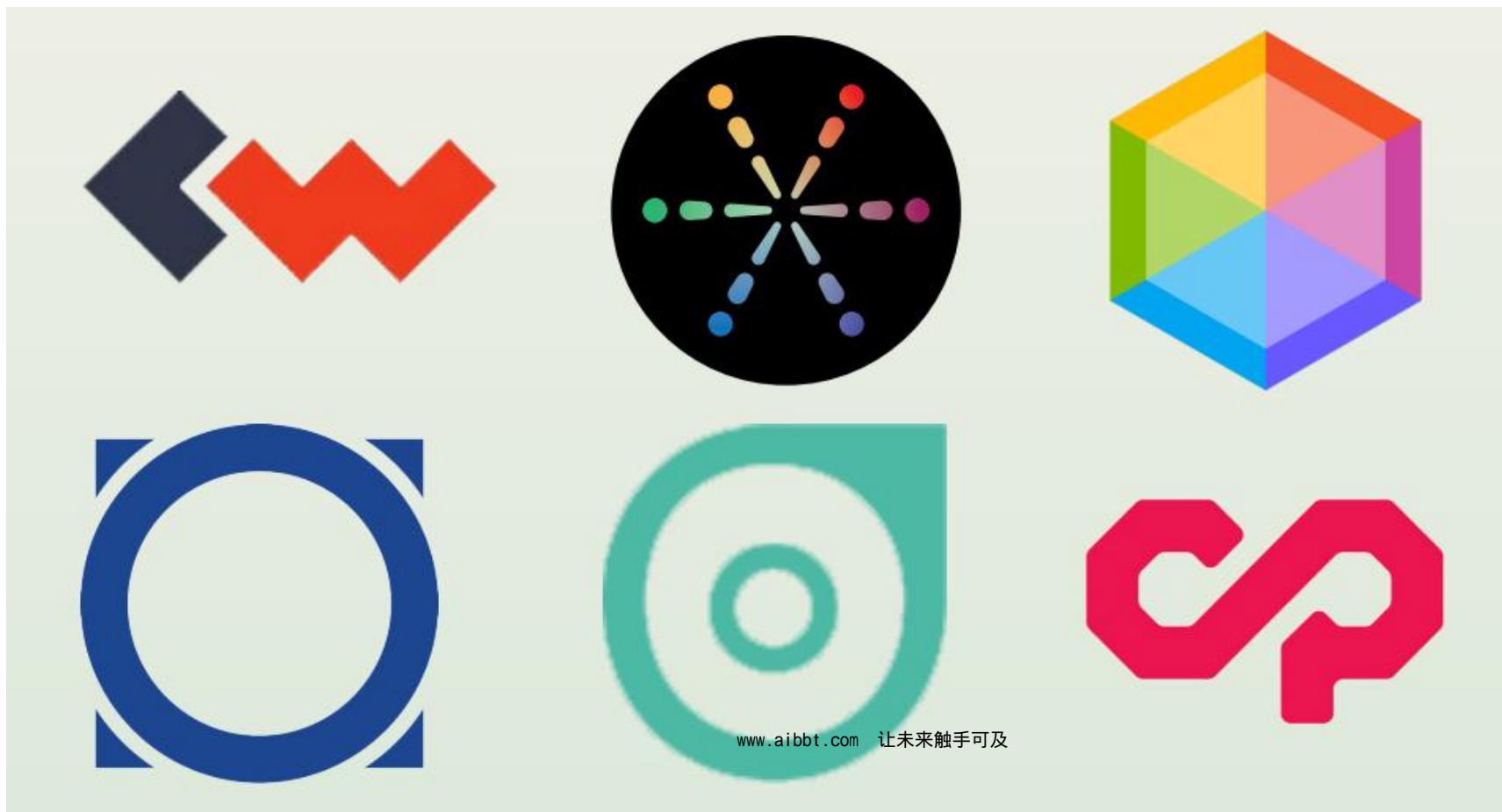
```
opReturn, err := builder.Script()  
msgtx.AddTxOut(wire.NewTxOut(0, opReturn))
```

锚定算法

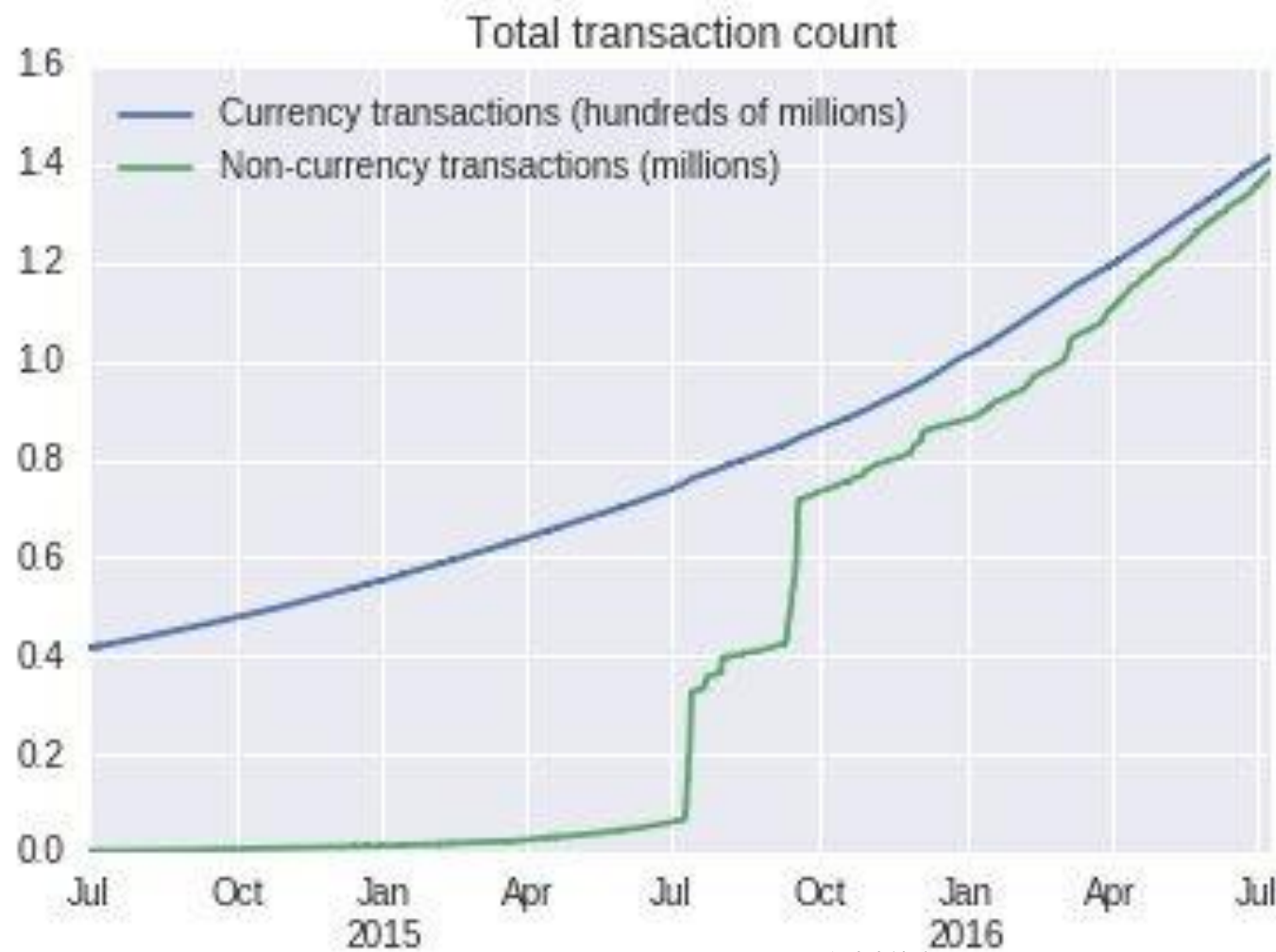
- Update UTXOs
 - Create New Tx
 - UTXO -> TXIn
 - Create TxOut, including OP_RETURN
 - Validate TX
 - Send Tx to network
-
- Wait for callback notification
 - Tx Confirmed (6 times, 20 times, etc)

OP_RETURN: Color Coins

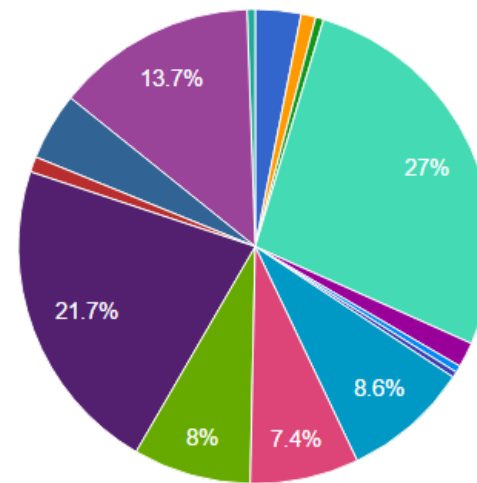
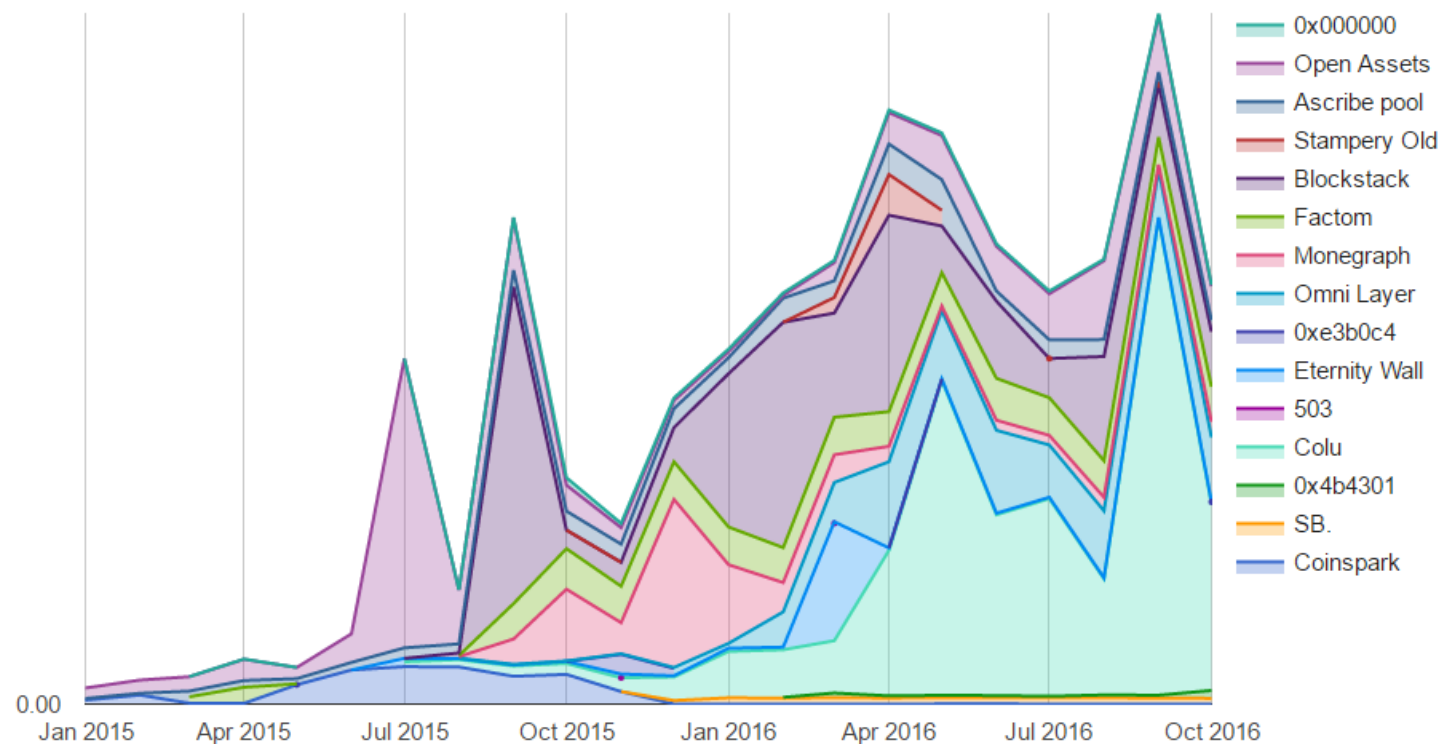
- 利用Op_return来发布数字资产



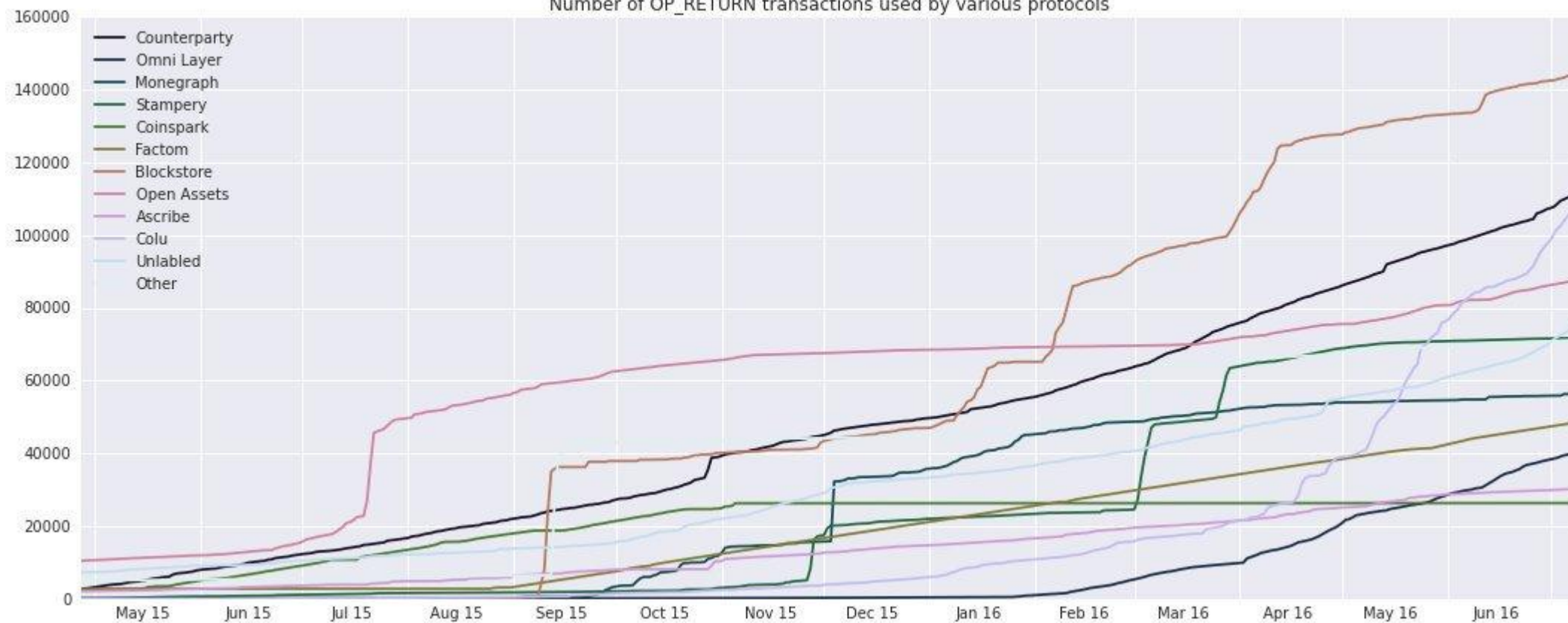
OP_RETURN 交易现状



OP_RETURN 交易（协议）



Number of OP_RETURN transactions used by various protocols

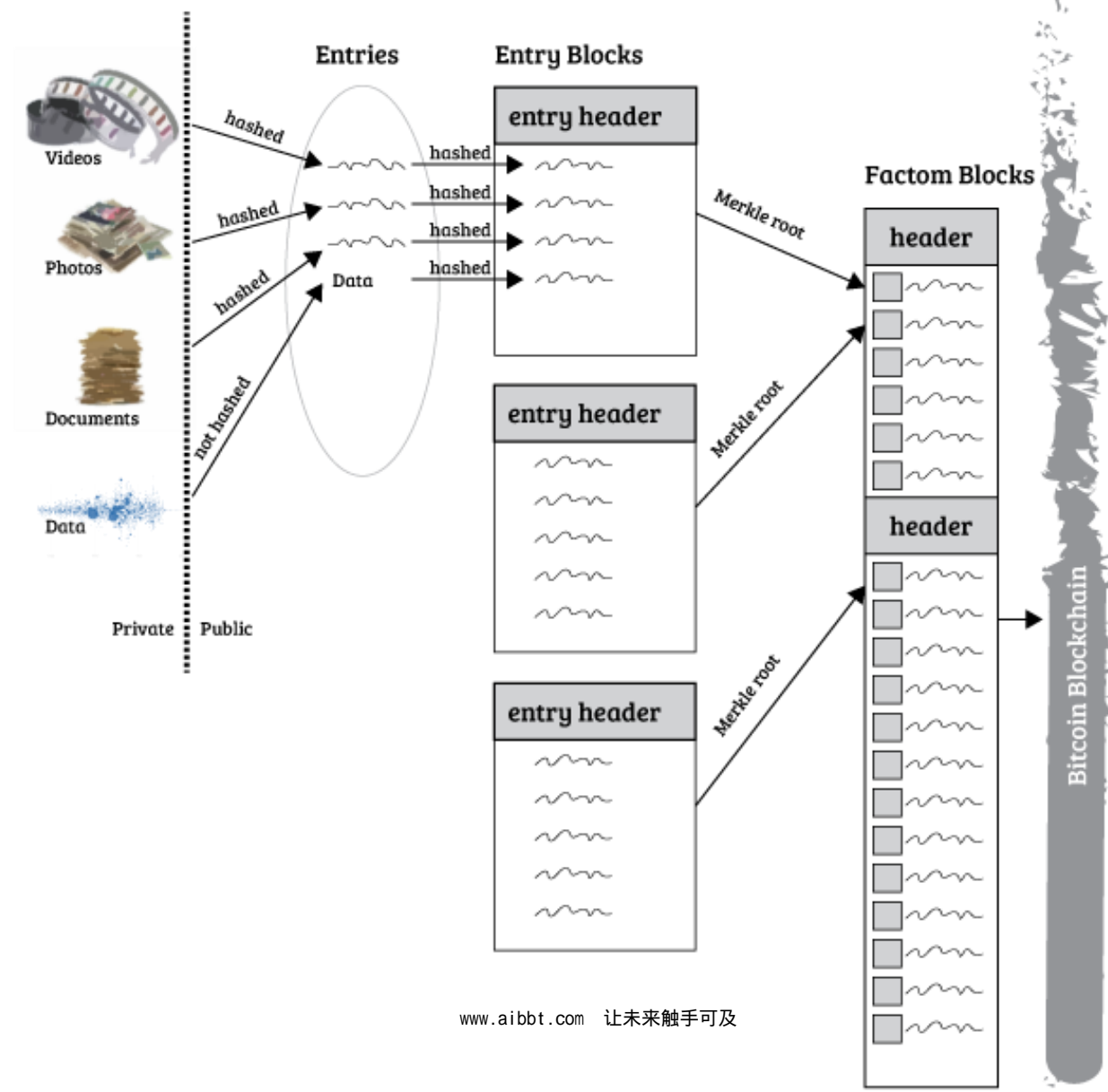


企业级的存证解决方案

- 成功的锚定
 - ✓交易不被收录、区块链的重组
- 锚定数据的语义和关联
 - ✓Encoding、
 - ✓数据之间的关系（版本、M:N）
 - ✓数据检索
- 交易的吞吐量和速度
- 隐私和权限控制

存证实例：Factom

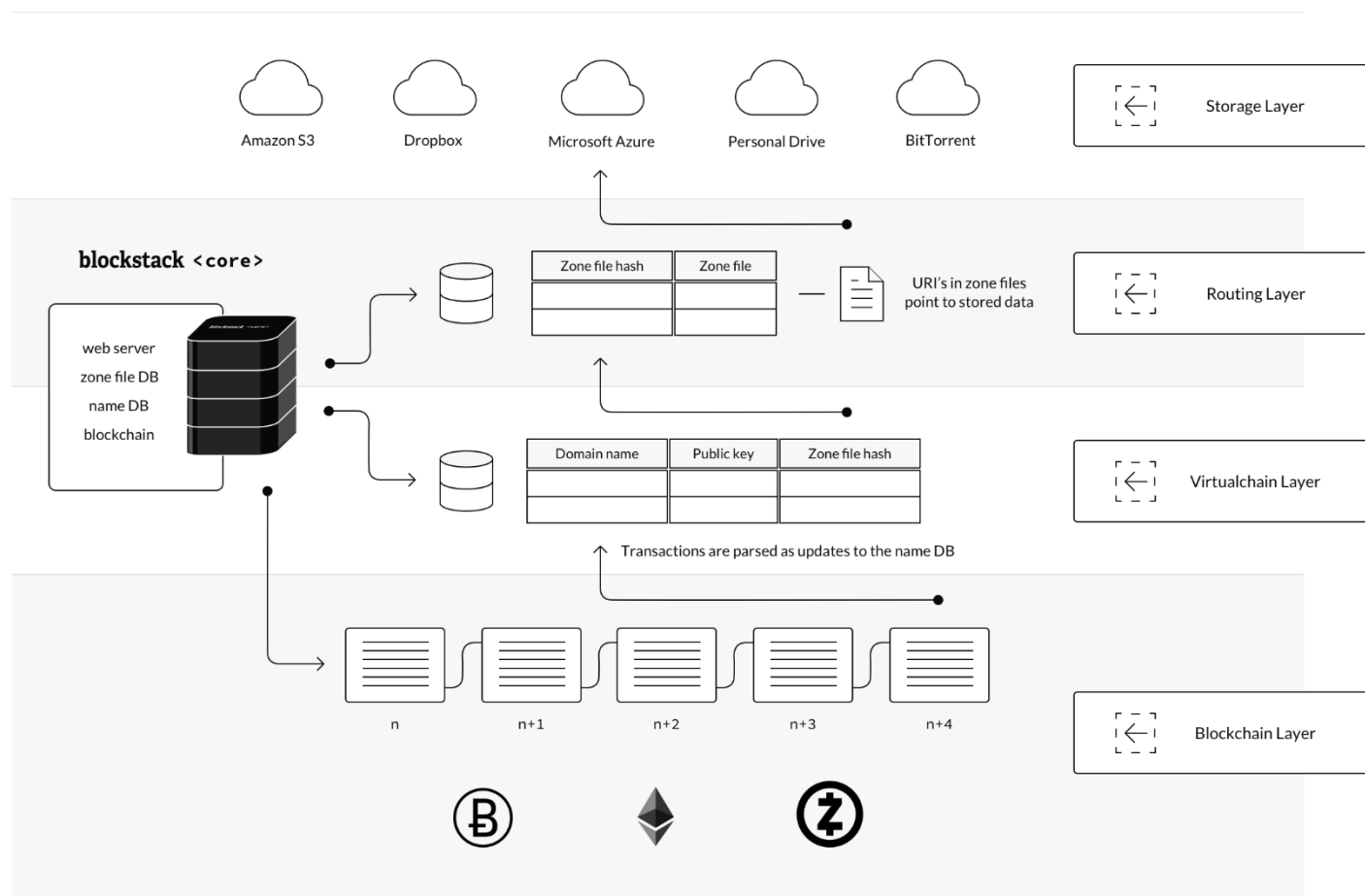
Complete Factom System



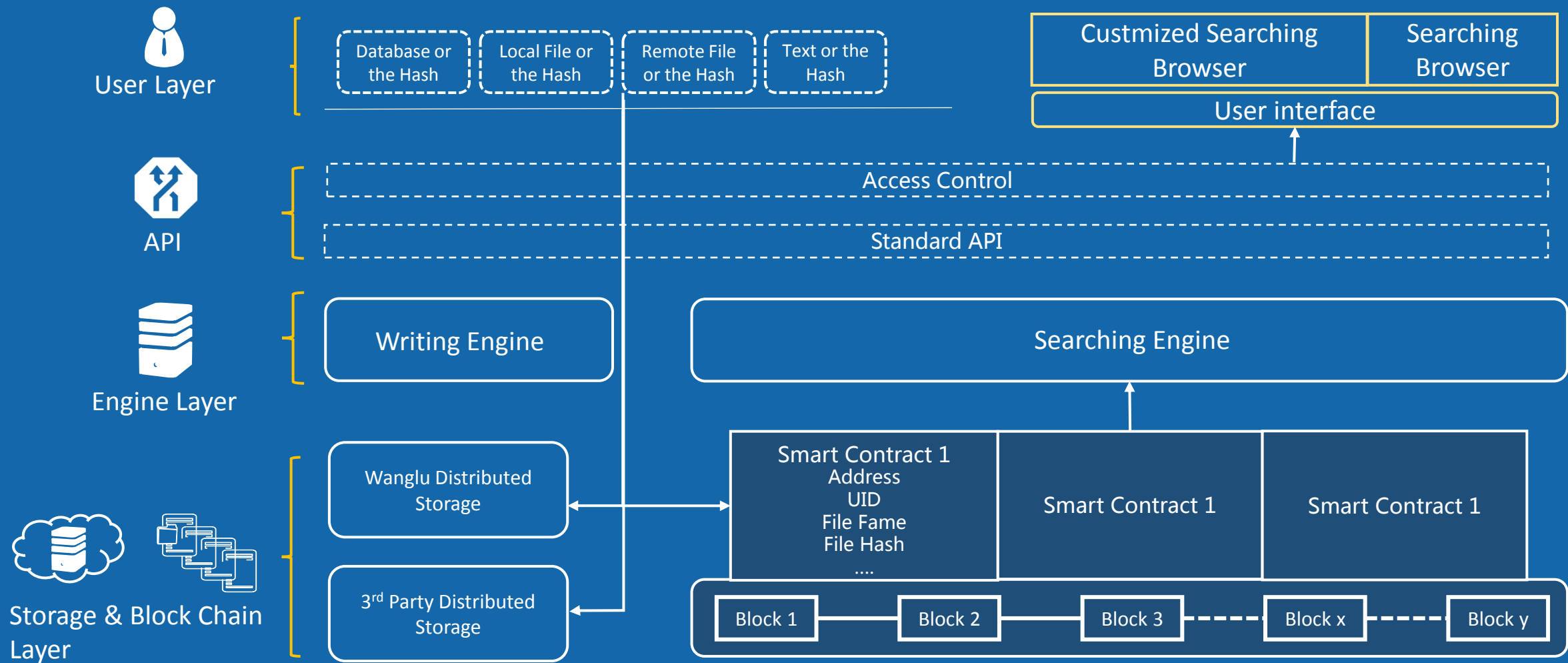
存证实例：blockstack

Blockstack Architecture

A platform for decentralized applications



存证实例：网录 (Walud)



谢谢！